UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,687	12/22/2000	Xun Wilson Huang	21816-04953	4655

758 7590 10/18/2006

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
ZHEN, LI B	

ART UNIT	PAPER NUMBER
2194	

DATE MAILED: 10/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,687	HUANG ET AL.	
	Examiner	Art Unit	
	Li B. Zhen	2194	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,16-32,36-52 and 56-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,16-19,21-32,36-39,41-52 and 56-58* is/are rejected.

7)☒ Claim(s) *20 and 40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 6/5/2006
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12,16-32,36-52 and 56-58 are pending in the application.

Response to Arguments

2. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Allowable Subject Matter

3. Claims 20 and 40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

4. The following is an examiner's statement of reasons for allowance:

The prior art of record does not expressly teach or render obvious the invention as recited in dependent claims 20 and 40 including all of the limitations of the base claim and intervening claims.

The prior art teaches a system for virtualizing user privileges [col. 4, lines 41 – 51 of Aziz] in a computer operating system including multiple virtual private servers [col. 4, lines 23 – 42 of Aziz], associating a user with a first virtual private server [col. 10, lines 15 – 25 of Aziz], the first virtual private server comprising a plurality of actual processes [col. 15, lines 30 – 42 of Aziz] executing within the same operating system as a second plurality of actual processes comprising a second virtual private server [col. 11, line 65 –

col. 12, line 9 of Aziz], designating a user as a virtual super-user [col. 10, lines 40-47 of Schneider], intercepting a call to the operating system for which actual super-user privileges are required, the call made by a process located in the operating system, the process owned by the user [col. 4, lines 41 – 54 of Aziz], granting privileges to the user [col. 11, lines 10 – 29 of Aziz], and allowing execution of the system call [col. 15, lines 30 – 42 of Aziz]. However, the prior art does not teach loading a system call wrapper, saving a pointer to the call to the operating system, wherein the pointer to the call to the operating system comprises a system call vector and replacing the pointer to the call to the operating system with a pointer to the system call wrapper, such that the system call wrapper is executed when the call to the operating system is invoked.

In addition, the prior art of record does not provide a basis of evidence for asserting a motivation that one of ordinary skill level in the art at the time the invention was made would have integrated or modified the system for virtualizing user privileges to include the features of: loading a system call wrapper, saving a pointer to the call to the operating system, wherein the pointer to the call to the operating system comprises a system call vector and replacing the pointer to the call to the operating system with a pointer to the system call wrapper, such that the system call wrapper is executed when the call to the operating system is invoked as recited in the context of dependent claims 20 and 40 including all of the limitations of the base claim and intervening claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-12, 16, 18, 21-32, 36, 38, 41-52, 56 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,779,016 to Aziz et al. [hereinafter Aziz] in view of U.S. Patent No. 6,785,728 to Schneider et al. [hereinafter Schneider, cited in the previous office action].

7. As to claim 1, Aziz teaches the invention substantially as claimed including a computer-implemented method for virtualizing user privileges [col. 4, lines 41 – 51] in a computer operating system including multiple virtual private servers [Each organization retains independent administrative control of its VSF; col. 4, lines 23 – 42], the method comprising:

associating a user with a first virtual private server [organization that owns or operates the VSF wants another server, and has added it through an administrative mechanism, such as a privileged Web page which allows it to add more servers to its VSF; col. 10, lines 15 – 25], the first virtual private server comprising a plurality of actual

processes [Web pages and security applications; col. 15, lines 30 – 42] executing within the same operating system as a second plurality of actual processes comprising a second virtual private server [OS provides a cluster file system that allows read/write access of a shared-disk partition between multiple nodes; col. 11, line 65 – col. 12, line 9];

intercepting a call to the operating system for which actual super-user privileges are required, the call made by a process located in the operating system, the process owned by the user [organization can access only the data and computing elements in the portion of the computing grid allocated to it, that is, in its VSF, even though it may exercise full (e.g. super-user or root) administrative access to these computers; col. 4, lines 41 – 54]; and

in response to the intercepted call to the operating system pertaining to the first virtual private server [provides administrative and management functions using a graphical user interface or other suitable user interface; col. 4, line 63 – col. 5, line 10]:

granting privileges to the user [CPU D is granted read-only access to data in a file system shared by the other Web servers in VSF 2; col. 11, lines 10 – 29]; and

allowing execution of the system call [VSF customer may be granted privileged access to create and modify its VSF itself; col. 15, lines 30 – 42]. Aziz does not specifically disclose designating a user as a virtual super-user and granting actual super-user privileges to the user.

However, Schneider teaches a virtual private network (VPN) 201 [col. 8, lines 22-50] designating a user as a virtual super-user [administrative policy 305 defines rights of

user groups to define/delete/modify objects in VPN 201; col. 10, lines 40-47], intercepting a call to the operating system for which actual super-user privileges are required [access filter 203 is thus able to control access by the user to the resource by interceding in the communication between a user and a service on the server which is able to provide the user with access to the information resource; col. 16, lines 15-36], granting actual super-user privileges to the user [Access filters 203 are designed such that the decision whether to grant a user access to an information resource need only be made in one of the access filters 203; col. 16, lines 33-50] and allowing execution of the system call [If the access is permitted, the message is once again encrypted and sent to access filter 403(5) nearest server 407; col. 17, line 37-col. 18, line 5].

It would have been obvious to a person of ordinary skill in the art at the time of the invention to apply the teaching of designating a user as a virtual super-user and granting actual super-user privileges to the user as taught by Schneider to the invention of Aziz because this provides scalable and decentralized administration of access to a virtual private network [col. 5, line 60-col. 6, line 7 of Schneider].

8. As to claim 2, Aziz teaches withdrawing the actual super-user privileges from the user after execution of the call to the operating system [col. 13, line 60 – col. 14, line 9].

9. As to claim 3, Aziz as modified teaches assigning a virtual super-user identifier to the user [col. 9, lines 39-50 of Schneider].

10. As to claim 4, Aziz as modified teaches the virtual super-user identifier comprises a super-user identifier and an indication of the first virtual private server [col. 9, lines 39-50 of Schneider].

11. As to claim 5, Aziz as modified teaches assigning a user identifier to the user and storing the user identifier and an indication of the first virtual private server in a virtual super-user list [database 301; col. 10, lines 19-48 of Schneider].

12. As to claim 6, Aziz as modified teaches assigning a super-user identifier to the user [col. 9, lines 39-50 of Schneider].

13. As to claim 7, Aziz teaches the intercepted call to the operating system comprises a call to the operating system for accessing a file [CPU D is granted read-only access to data in a file system shared by the other Web servers in VSF 2; col. 11, lines 10 – 30].

14. As to claim 8, Aziz as modified teaches the intercepted call to the operating system pertains to the virtual private server associated with the user when the file to be accessed is associated with the virtual private server [col. 26, lines 19-28 of Schneider].

15. As to claim 9, Aziz teaches the intercepted call to the operating system comprises a call to the operating system for terminating a process [col. 13, line 60 – col. 14, line 9].

16. As to claim 10, Aziz teaches the intercepted call to the operating system pertains to the first virtual private server when the process to be terminated is associated with the first virtual private server [Once the CPU has shut down, the Control Plane removes ports v8 and v9 from VLAN 2; col. 11, lines 1 – 12].

17. As to claim 11, Aziz teaches identifying each process associated with the first virtual private server, and terminating each identified process [col. 11, lines 1 – 12].

18. As to claim 12, Aziz as modified teaches a data structure stores associations between processes and virtual private servers, and identifying each process by its association with the first virtual private server in the data structure [database 301; col. 10, lines 19-48 of Schneider].

19. As to claim 16, Aziz teaches responsive to the intercepted call to the operating system not pertaining to the first virtual private server, disallowing execution of the call to the operating system [firewall configuration protects CPUs B and C against unauthorized access; col. 9, line 60 – col. 10, line 6].

20. As to claim 18, Aziz teaches allowing comprises: executing the call to the operating system [VSF customer may be granted privileged access to create and modify its VSF itself; 15, lines 30 – 42].

21. As to claims 21-32, 36 and 38, these are product claims that correspond to method claims 1-12, 16 and 18; note the rejections to claims 1-12, 16 and 18 above, which also meet these product claims.

22. As to claims 41-52, 56 and 58, these are system claims that correspond to method claims 1-12, 16 and 18; note the rejections to claims 1-12, 16 and 18 above, which also meet these systems claims.

23. Claims 17, 19, 37, 39, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz and Schneider further in view of U.S. Patent NO. 6,658,571 to O'Brien [cited in previous office action].

24. As to claim 17, Aziz as modified does not teach disallowing execution of a system call for inserting a module into an operating system kernel.

However, O'Brien teaches responsive to the intercepted system call comprising a system call for inserting a module [malicious software] into an operating system kernel, disallowing execution of the system call [each security module 105 "wraps" one or more applications 107 in the sense that applications 107 cannot access computing resources

106 for which they are unauthorized in the event that an application 107 executes malicious software; col. 3, lines 39 – 56].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to disallow the execution of a system call for inserting a module into an operating system kernel as taught by O'Brien to the invention of Aziz as modified by Schneider because this prevents malicious software from damaging computing resources that user is not normally allowed to access [col. 4, lines 33 – 37 of O'Brien].

25. As to claim 19, Aziz as modified teaches loading a system call wrapper [Security modules 105 are kernel-loadable modules that make and enforce application-specific or resource-specific policy decisions for applications 107; col. 3, lines 38 – 56 of O'Brien], saving a pointer to the system call [each entry includes the following fields: a pointer to the original system call handler within the operating system; col. 5, lines 27 – 46 of O'Brien] and replacing the pointer to the system call with a pointer to the system call wrapper, such that the system call wrapper is executed when the system call is invoked [for each system call being wrapped, security master 103 redirects each pointer from the standard handler within the operating system to a corresponding system call wrapper within security master 103; col. 5, lines 27 – 46 of O'Brien].

26. As to claim 39, this is similar in scope to claim 19; therefore, claim 39 is rejected for the same reasons as claim 19.

27. As to claims 37 and 57, they are similar in scope to claim 17; therefore, claims 37 and 57 are rejected for the same reasons as claim 17 above.

Conclusion

28. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

CONTACT INFORMATION

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Li B. Zhen whose telephone number is (571) 272-3768. The examiner can normally be reached on Mon - Fri, 8:30am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Thomson can be reached on 571-272-3718. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Li B. Zhen
Examiner
Art Unit 2194

LBZ

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER